POSTAL SE

Privacy Act of 1974; System of Records

AGENCY: Postal Service™.

ACTION: Notice of a new system of records.

SUMMARY: The United States Postal Service (USPS™) is proposing to create a new General Privacy Act System of Records.

DATES: This new System of Records will become effective without further notice on **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**, unless comments received on or before that date result in a contrary determination.

ADDRESSES: Comments may be submitted via email to the Privacy and Records Management Office, United States Postal Service Headquarters (privacy@usps.gov). Arrangements to view copies of any written comments received, to facilitate public inspection, will be made upon request.

FOR FURTHER INFORMATION CONTACT: Janine Castorina, Chief Privacy and Records Management Officer, Privacy and Records Management Office, 202-268-3069 or privacy@usps.gov.

SUPPLEMENTARY INFORMATION:

Background

The world of commercial information technology resources (“IT”) is constantly changing and innovating to improve the daily lives of businesses, their employees, and their customers. This pace can often result in unanticipated obsolescence, necessitating review of an organization’s already implemented solutions. For the Postal Service, legal processes and notice required by the Privacy Act present additional challenges, as new technologies will require further review for possible compliance issues to meet statutory and regulatory requirements.

To better meet the changing technology world, the Postal Service will consolidate existing Systems of Records (“SOR”s) covering IT into three new, comprehensive Systems of Records. These SORs will work in tandem, with each individual SOR covering a specific group of related functions, and all three SORs working together to support a seamless technology experience.

These SORs, generally, will cover the following three areas:

- Infrastructure, covering records created for use throughout the entirety of a particular IT resource in addition to covering the records created from the usage of those records by users and applications.
- Applications, covering records created through the regular use of an application.
- Administrative, covering records created for monitoring and administration of users and applications within an IT resource.

In addition to covering these three areas generally, the Postal Service will look ahead in an effort to include possible future technology solutions within this System of Records. This will give the Postal Service flexibility to more easily adapt to the advancing pace of information technology and to better fulfill its service obligations. This will also provide transparency into the collection of records relating to commercial IT, allowing Postal employees, contractors, and the public to more easily identify what we do with their information.

Rationale for the creation of a new USPS System of Records

Currently, records relating to the implementation of IT resources are housed primarily in USPS 500.000, Property Management Records, with other IT-related components appearing in USPS 890.000, Sales, Marketing, Events, and Publications and other SORs. SOR 500.000 reflects not only IT access records, but also building access and related records. This results in a mixture of uses within SOR 500.000, which reduces optimization and can result in confusion.

The creation of a new SOR to encompass commercial IT resources, therefore, provides a platform which is easy to understand and allows for greater flexibility in use and maintenance. Since the new SOR will house only IT resources, the public can more easily understand what information is collected and how it is used.

Further, documenting IT records within one SOR provides for greater flexibility in adding new resources as well as maintaining existing resources. For example, one application may already collect and store, for the same purpose, data elements that a new application will use. With a record already documented, the implementation process of the new technology will be

streamlined while also meeting statutory and regulatory mandates.

Description of New or Modified System of Records

This new system of records is being developed to support the implementation of various commercial IT resources and to provide support for future implementations.

This system specifically will cover categories of records referred to collectively as "Infrastructure." Categories of Records in this system reference data elements created in one application and passed through to multiple applications. This SOR also contains Categories of Records that reference transformations or analysis of those data elements resulting from interactions with users or applications. Data elements documented within this system may be passed through or referenced by records otherwise contained in systems USPS 550.100 Commercial Information Technology Resources- Applications and USPS 550.200 Commercial Information Technology Resources - Administrative; therefore, those elements will not be specifically documented within those systems unless those systems utilize those elements in a transformative manner.

This System of Records may overlap with elements appearing in other Systems of Records, as indicated in the Rationale for Changes to USPS System of Records section. This new System of Records will encompass commercially developed or commercially assisted IT resources. Applications developed in-house or by the Postal Service, such as Informed Delivery®, will still be represented in their own SOR.

SYSTEM NAME AND NUMBER:

550.000 Commercial Information Technology Resources- Infrastructure

SECURITY CLASSIFICATION:

None.

SYSTEM LOCATION:

All USPS facilities and contractor sites.

SYSTEM MANAGER(S):

Chief Information Officer and Executive Vice President, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

39 U.S.C. 401, 403, and 404.

PURPOSE(S) OF THE SYSTEM:

1. To provide USPS employees, contractors, and other authorized individuals with hierarchical access to and accounts for commercial information technology resources administered by the Postal Service and based on least privileged access.
2. To facilitate a cohesive software experience and simplify ease of use by sharing user and application data across participating IT programs.
3. To authenticate user identity for the purpose of accessing USPS information systems.
4. To assess user attributes and assign related access privileges.
5. To authenticate suppliers and contractors and facilitate further access to downstream Postal Service information systems.
6. To provide active and passive monitoring of information systems, applications, software, devices, and users for information security risks.
7. To review information systems, applications, software, devices, and users to ensure compliance with USPS regulations.
8. To facilitate and support cybersecurity investigations of detected or reported information security incidents.
9. To administer programs, processes, and procedures to assess information security risks and to detect information security threats and vulnerabilities.
10. To provide tools and analytics for USPS employees and contractors to measure work productivity and improve efficiency.
11. To improve manager-subordinate relationships within their formal reporting structure through data-based insights generated from their own email and related electronic communications with subordinates.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

1. Individuals with authorized access to USPS computers, information resources, and facilities, including employees, contractors, business partners, suppliers, and third parties.

2. Individuals participating in web-based meetings, web-based video conferencing, web-based communication applications, and web-based collaboration applications.

CATEGORIES OF RECORDS IN THE SYSTEM:

1. *Information System Account Access records*: Records relating to the access or use of an information system, application, or piece of software, including; Name, User ID, Email Address, User Type, User Role, Job Title, Department, Manager, Company, Street Address, State Or Province, Country Or Region, Work Phone Number(s), Employee Identification Number (EIN), Advanced Computing Environment (ACE) ID, License Information, Action Initiated, Datetime, User Principle Name, Usage Location, Alternate Email Address, Proxy Address, Age Group**,** IP Address, MAC Address, Password, Multi-Factor Authentication Credentials, Security Questions, Security Answers, Passcode, Geolocation Data, User Profile Picture, Picture Metadata, Information Technology Account Administration User Configuration Status, Supplier Credentials, Supplier Company Codes, Conditional Access Attributes.
2. *Security Analytics records*: Records relating to the gathering, analysis, review, monitoring, and investigation of information system security risks, including; User Investigation Priority Score, User Identity Risk Level, User Lateral Movement Paths, User Devices Numbers, User Account Numbers, User Resources Numbers, User Locations Numbers, User Matches Files Numbers, User Locations, Apps Used By User, User Groups, User Last Seen Date, User Affiliation, User Domain, App Instance, Organizational Groups, User Account Status, Activity ID, Activity Objects, Activity Type, Administrative Activity, Alert ID, Applied Action, Activity Date, Device Tag, Activity Files And Folders, Impersonated Activities, App Instance Activity, App Location Activity, Activity Matched Policy, Activity Registered ISP, Activity Source, Activity User, Activity User Agent, Activity User Agent Tag, Application Risk Score, Application Activity, User Software Deactivation, User Software Installation, User Software Removal, Last Date Of Software Execution, Internet Application Transaction Counts, Data Volume Upload, Data Volume Download, Data Sensitivity Classification, Internet Protocol, Internet Port, Internet Access History.

3. *Productivity Analytics records*: Records relating to the gathering, analysis, review, and investigation of information system utilization, including; Calendar Appointments, Email Read Rate, Email Response Rate, Operating System Activity History, Email Timestamp, Statements Made In Email Body, Email Sender, Email Recipient, Email Subject Line, Calendar Event Type, Calendar Event Status, Calendar Event Category, Calendar Event Subject, Calendar Event Duration, Calendar Event Attendees, Meeting Organizer, Meeting Invitees, Meeting Subject Line, Meeting Scheduled Time, Meeting Attendee Status, Meeting Scheduled Location, Web Call Organizer, Web Call Invitees, Web Call Scheduled Time, Web Call Joined Time, Web Call Duration, Web Call Status, Web Call Join Status, Number Of Collaborative Audio Calls Made, Number Of Collaborative Video Calls Made, Chat Initiator, Chat Recipient, Chat IM Sent Time, Number Of Cloud-Based Personal Storage Documents Worked On, Number Of Cloud-Based Enterprise Storage Documents Worked On, Device Name.

RECORD SOURCE CATEGORIES:

Employees; contractors; suppliers; customers.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

Standard routine uses 1. through 9. apply. In addition:

a) Disclosure of records to appropriate agencies, entities, and persons when (1) the Postal Service suspects or has confirmed that there has been a breach of the system of records; (2) the Postal Service has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Postal Service (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Postal Service's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Automated database, computer storage media, and paper.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

1. Records relating to information system access are retrievable by name, email address, username, geolocation data, and ACE ID.
2. Records relating to security analysis are retrievable by name, unique user ID, email address, geolocation data, IP address and computer name.
3. Records relating to productivity are retrievable by name, email address, and ACE ID.
4. Records relating to third-parties are retrievable by name, email address, user name, and IP address.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

1. Records relating to information system access are retained twenty-four months after last access.
2. Records relating to security analysis are retained for twenty-four months.
3. Records relating to productivity are retained for twenty-four months.
4. Records relating to third-parties are retained for twenty-four months.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Paper records, computers, and computer storage media are located in controlled-access areas under supervision of program personnel. Computer access is limited to authorized personnel with a current security clearance, and physical access is limited to authorized personnel who must be identified with a badge.

Access to records is limited to individuals whose official duties require such access. Contractors and licensees are subject to contract controls and unannounced on-site audits and inspections. Computers are protected by encryption, mechanical locks, card key systems, or other physical access control methods. The use of computer systems is regulated with installed security software, computer logon identifications, and operating system controls including access controls, terminal and transaction logging, and file management software.

RECORD ACCESS PROCEDURES:

Requests for access must be made in accordance with the Notification Procedure above and USPS Privacy Act regulations regarding access to records and verification of identity under 39 CFR 266.5.

CONTESTING RECORD PROCEDURES:

See Notification Procedure and Record Access Procedures above.

NOTIFICATION PROCEDURES:

Customers wanting to know if other information about them is maintained in this system of records must address inquiries in writing to the Chief Information Officer and Executive Vice President and include their name and address.

EXEMPTION PROMULGATED FROM THIS SYSTEM:

None.

HISTORY:

None.

Joshua J. Hofer,

Attorney, Ethics & Legal Compliance.

[FR Doc. 2021-09755 Filed: 5/7/2021 8:45 am; Publication Date: 5/10/2021]